CSCE 222
Discrete Structures for Computing

Introduction to Proofs

Dr. Philip C. Ritchey

Some Definitions

- **Theorem**
  - A statement that can be shown to be true
- **Proof**
  - A valid argument that establishes the truth of a theorem
- **Direct Proof**
  - Prove $p \rightarrow q$, $\forall x\, P(x) \rightarrow Q(x)$ by assuming that p is true and using the rules of inference to show that q must also be true.

Example

- **Theorem**
  - If x, y are odd integers, then $x \cdot y$ is odd
- **Proof**
  - Let x, y be odd integers. Then,
  - $\exists a\ x = 2a + 1$
  - $\exists b\ y = 2b + 1$
  - $x \cdot y = (2a + 1)(2b + 1)$
  - $x \cdot y = 4ab + 2a + 2b + 1$
  - $x \cdot y = 2(2ab + a + b) + 1$
  - $\therefore\ x \cdot y$ is odd □

Indirect Proofs (not direct)

- **Proof by Contraposition**
  - Want $p \rightarrow q$
  - Show $\neg q \rightarrow \neg p$
- Theorem: Let n be an integer. **If $\boldsymbol{n^3 + 13}$ is odd, then $\boldsymbol{n}$ is even**.
  - Proof: Show that n odd $\rightarrow n^3 + 13$ even.
  - **Assume $\boldsymbol{n}$ is odd**
  - $n = 2a + 1$
  - $n^3 + 13 = (2a + 1)^3$
  - $n^3 + 13 = 8a^3 + 12a^2 + 6a + 14$
  - $n^3 + 13 = 2(4a^3 + 6a^2 + 3a + 7)$
  - $\therefore n^3 + 13$ is even
  - It follows that **if $\boldsymbol{n^3 + 13}$ is odd, then $\boldsymbol{n}$ is even** □

Indirect Proofs (not direct)

- Proof by Contradiction
  - Trying to prove p
  - Prove by showing $\neg p \rightarrow (r \wedge \neg r)$
    - Thus, $\neg p \equiv F \Rightarrow p \equiv T$
- Theorem: If $x + y \geq 2$, then $x \geq 1$ or $y \geq 1$
  - Proof: Assume $\neg\Big((x + y \geq 2) \rightarrow \big((x \geq 1) \vee (y \geq 1)\big)\Big)$
  - $(x + y \geq 2) \wedge \neg\big((x \geq 1) \vee (y \geq 1)\big)$
  - $(x + y \geq 2) \wedge \big((x < 1) \wedge (y < 1)\big)$
  - $x + y < 1 + 1$
  - $x + y < 2$ contradicts $x + y \geq 2$
  - $\therefore \neg\neg\Big((x + y \geq 2) \rightarrow \big((x \geq 1) \vee (y \geq 1)\big)\Big)$ $\square$

Proof that $\sqrt{2}$ is irrational

- Prove that $\sqrt{2}$ is irrational.
  - $\left(\exists p, q\ \left((q \neq 0) \land \left(r = \frac{p}{q}\right)\right)\right) \rightarrow r$ is **rational**
  - Ex: 1.5 = 3/2 = 6/4
  - A real number which is not rational is **irrational.**

Proof that $\sqrt{2}$ is irrational

- Proof by contradiction
  - Suppose $\sqrt{2}$ is rational
  - Then, there exist integers a, b such that $b \neq 0$ and $\sqrt{2} = \frac{a}{b}$, where a, b have no common factors
  - $\left(\sqrt{2}\right)^2 = \left(\frac{a}{b}\right)^2$
  - $2 = \frac{a^2}{b^2}$
  - $2b^2 = a^2$, thus a is even
  - $2b^2 = (2k)^2$
  - $b^2 = 2k^2$, thus b is even
  - If both are even, then they share a common factor. This contradicts the assumption that $\sqrt{2}$ is rational.
  - Therefore $\sqrt{2}$ is **NOT** rational

Proofs of Equivalence

- To prove $p \leftrightarrow q$
  - Show $p \rightarrow q$ **and** $q \rightarrow p$
- Prove that p and q are equivalent
  - p: n is even
  - q: n^2 is even
- $p \rightarrow q$
  - Assume n is even.
  - $n = 2k$
  - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ □
- $q \rightarrow p$
  - Use contrapositive: $\neg p \rightarrow \neg q$
  - Assume n is odd
  - $n = 2k + 1$
  - $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
- $\therefore p \leftrightarrow q$ □

Counterexamples

- To prove $\neg \forall x P(x)$
  - Find **counterexample** x that satisfies $\neg P(x)$
  - Show $\exists x \neg P(x)$
- Show that not every positive integer is the sum of the squares of 2 integers.
  - Proof: the counterexample is 3